PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-005859
(43)Date of publication of application : 08.01.2003

(51)Int.Cl. G06F 1/00
G06F 9/445
G06F 15/00

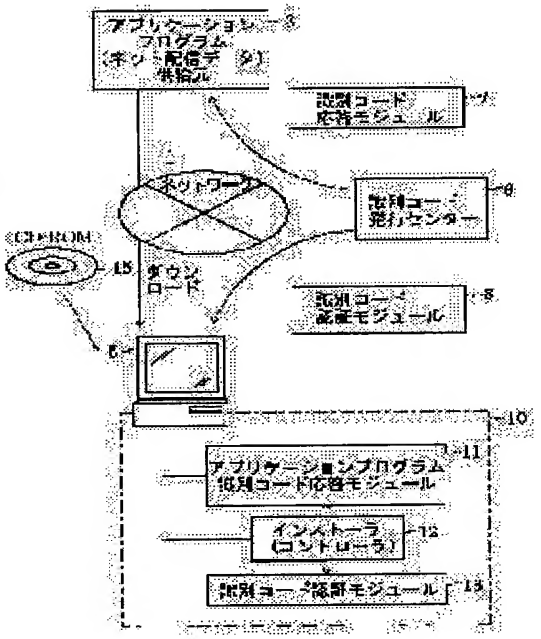
(21)Application number : 2001-216467
(22)Date of filing : 17.07.2001

(71)Applicant : SUMIYA YUICHI
(72)Inventor : SUMIYA YUICHI

(30)Priority
Priority number : 2001116516 Priority date : 16.04.2001 Priority country : JP

(54) METHOD FOR MANAGING PROGRAM AND DATA, AND COMPUTER

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent an application program from being unauthorizedly copied by preventing the application program from being installed by any one other than a client who has made an official purchase agreement for the program.
SOLUTION: Even when the application program and data are downloaded to a terminal 5, it is made impossible to use them as they are. Unique identification codes that do not overlap on one another are allocated to all application programs, and an identification code response module 7 that responds with the identification codes as a key is incorporated into the application program, the program is provided to an application program supply source 3. An identification code authentication module 8 executes an authentication processing responding to an identification code authentication module 13 in a terminal 5.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision

of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－5859
（P2003－5859A）
(43)公開日　平成15年１月８日(2003.1.8)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　1/00		Ｇ０６Ｆ　15/00	３３０Ａ	５Ｂ０７６
9/445		9/06	６６０Ｇ	５Ｂ０８５
15/00	３３０		６４０Ａ	
			６１０Ｌ	

審査請求　未請求　請求項の数14　ＯＬ　（全 16 頁）

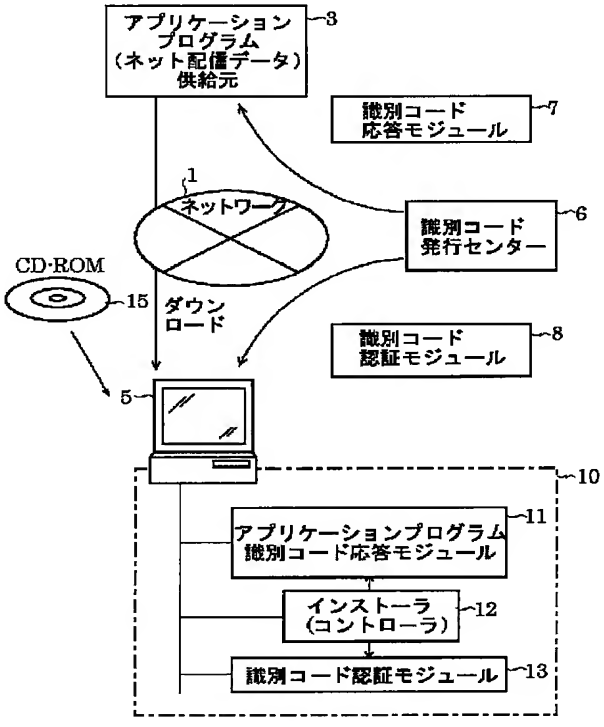
(21)出願番号　特願2001－216467(P2001－216467)
(22)出願日　平成13年７月17日(2001.7.17)
(31)優先権主張番号　特願2001－116516(P2001－116516)
(32)優先日　平成13年４月16日(2001.4.16)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　301038726
角谷　優一
東京都杉並区高井戸東３丁目14番29号
(72)発明者　角谷　優一
東京都杉並区高井戸東３丁目14番29号
(74)代理人　100102923
弁理士　加藤　雄二

Ｆターム(参考)　5B076 BB06 FB02
5B085 AA08 AE23 BG06

(54)【発明の名称】　プログラムやデータの管理方法とコンピュータ

(57)【要約】
【解決手段】　アプリケーションプログラムやデータを端末５にダウンロードしても、そのままでは使用できないようにする。全てのアプリケーションプログラムに対し、互いに重複しないユニークな識別コードを割り付、その識別コードをキーとして応答する識別コード応答モジュール７を組み込む。アプリケーションプログラム供給元３に対して提供する。識別コード認証モジュール８は、端末５において、識別コードに応答して認証処理を実行する。
【効果】　正式にプログラムの購入契約をしたクライアント以外はアプリケーションプログラムのインストールができないので、不正コピーを防止できる。



【特許請求の範囲】

【請求項１】　コンピュータ上で動作するアプリケーションプログラムに、重複しないユニークな識別コードを割り付けた識別コード応答モジュールを含めておくとともに、

前記アプリケーションプログラムをインストールされるコンピュータ上で、前記識別コードと同一の識別コードを割り付けた識別コード認証モジュールを動作させ、

この識別コード認証モジュールと前記識別コード応答モジュールの通信により識別コードの一致が確認されたときにのみ、インストーラに前記アプリケーションプログラムのインストールを実行させることを特徴とするアプリケーションプログラムのインストール管理方法。

【請求項２】　コンピュータにダウンロードされる任意のデータ群に、重複しないユニークな識別コードを割り付けた識別コード応答モジュールを含めておくとともに、

前記データ群をダウンロードされるコンピュータ上で、前記識別コードと同一の識別コードを割り付けた識別コード認証モジュールを動作させ、

この識別コード認証モジュールと前記識別コード応答モジュールの通信により識別コードの一致が確認されたときにのみ、コントローラに前記データ群のダウンロードを実行させることを特徴とするデータ群のダウンロード管理方法。

【請求項３】　予めコンピュータに登録されたアプリケーションプログラムが、予めそのコンピュータに登録された識別コードを付加したコマンドを発行した場合にのみ、そのコンピュータ上での当該コマンドの実行を許可する識別コード認証モジュールを備えたことを特徴とするコンピュータ。

【請求項４】　請求項３に記載のコンピュータにおいて、

識別コード認証モジュールは、任意のタイミングで、アプリケーションプログラムに対して登録された識別コードを別の識別コードに更新することを特徴とするコンピュータ。

【請求項５】　一定の重複しないユニークな識別コードであって、予め登録したものを付加したデータを使用したアクセスのみを許可するデータアクセス管理モジュールを備えたことを特徴とするコンピュータ。

【請求項６】　コンピュータと所定の情報交換処理を実行する媒体に、重複しないユニークな識別コードを割り付けた識別コード応答モジュールを含めておくとともに、

前記媒体を前記コンピュータに接続したとき、前記媒体に対応する識別コードをコンピュータに登録して管理する識別コード認証モジュールをコンピュータ上で動作させ、

この識別コード認証モジュールと前記識別コード応答モジュールの通信により、媒体中の識別コード応答モジュールに割りつけられた識別コードと、その媒体に対応する登録された識別コードの一致が確認されたときにのみ、前記情報交換処理を実行させることを特徴とする情報交換処理の管理方法。

【請求項７】　請求項６に記載の管理方法において、

識別コード認証モジュールは、情報交換処理が終了したタイミングで、前記媒体の識別コード応答モジュールを、これまでとは別のユニークな新たな識別コードを割り付けたものに更新するとともに、コンピュータにその新たな識別コードを、当該媒体に対応するものとして登録することを特徴とする情報交換処理の管理方法。

【請求項８】　コンピュータにインストールしようとする情報が記録された記憶媒体には、認証用データをやりとりして認証処理を実行する機能を持つ応答モジュールが記録され、

前記情報をインストールするコンピュータは、前記応答モジュールと認証用データをやりとりして認証処理を実行する機能を持つ認証モジュールと、認証処理が正常に終了したとき、前記記憶媒体に記憶された情報をコンピュータにインストールするインストーラとを備え、

少なくとも前記認証モジュールは、ネットワークを通じて認証モジュール配信用サーバからダウンロードされることを特徴とする情報のコンピュータへのインストール方法。

【請求項９】　請求項８に記載のインストール方法において、

認証モジュール配信用サーバに対して認証モジュールのダウンロードを要求する機能を持つ配信要求モジュールを備えることを特徴とする情報のコンピュータへのインストール方法。

【請求項１０】　請求項８に記載のインストール方法において、

認証モジュール配信用サーバには、認証モジュールの配信履歴データを記録する配信記録部が備えられていることを特徴とする情報のコンピュータへのインストール方法。

【請求項１１】　請求項８に記載のインストール方法において、

認証モジュールは、コンピュータに正常に情報のインストールが終了すると無効化されることを特徴とする情報のコンピュータへのインストール方法。

【請求項１２】　カードを使用して自動的に所定の取引を実行する自動取引装置において、

前記カードには、入力データを所定のアルゴリズムで変換して識別コードを発生する第１の識別コード発生モジュールと、この第１の識別コード発生モジュールの出力する識別コードを保持して、次のタイミングで、保持していた識別コードを前記第１の識別コード発生モジュールに入力する第１の識別コードレジスタとが設けられ、

3

前記ＡＴＭには、入力データを前記第１の識別コード発生モジュールと同一のアルゴリズムで変換して識別コードを発生する第２の識別コード発生モジュールと、この第２の識別コード発生モジュールの出力する識別コードを保持して、次のタイミングで、保持していた識別コードを前記第２の識別コード発生モジュールに入力する第２の識別コードレジスタと、前記第１の識別コード発生モジュールの出力した識別コードと前記第２の識別コード発生モジュールの出力した識別コードとが一致したかどうかを判定して認証処理をする認証モジュールが設けられ定ることを特徴とする自動取引装置の認証処理方法。

【請求項１３】　請求項１２に記載の自動取引装置の認証方法において、

前記第１の識別コード発生モジュールは、認証処理開始直前に入力されたパスワードと第１の認証コードレジスタに保持された認証コードを受け入れて、新たな認証コードを発生し、

前記第２の識別コード発生モジュールは、認証処理開始直前に入力されたパスワードと第２の認証コードレジスタに保持された認証コードを受け入れて、新たな認証コードを発生することを特徴とする自動取引装置の認証処理方法。

【請求項１４】　コンピュータに設けられた監視モジュールであって、予め管理テーブルに認証コードが登録されたアプリケーションによる要求のみをオペレーティングシステムに伝えるように動作し、ネットワークに接続されたネットワークインターフェイスを通じて、予め特定された記憶領域にデータが書き込まれる処理は前記監視モジュールの監視外に置くように、コンピュータを動作させるコンピュータプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はコンピュータにインストールするプログラムやコンピュータに記憶させるデータファイルなどの安全性や信頼性を確保するプログラムやデータの管理方法とこの管理を実行するコンピュータに関する。

【０００２】

【従来の技術】

【０００３】コンピュータシステムで、セキュリティを脅かすものには、情報の盗聴、システムやプライベートなネットワークへの侵入、本人のなりすまし、データの改竄、データやシステムの破壊といったのものがあげられる。コンピュータをインターネットに接続して、情報の入手、発信、やり取り等を行うということは、プライベートな自らのネットワークやコンピュータシステムを不特定多数の者に開放して、アクセスされる危険にさらすことになる。また、自分からの情報を見ず知らずの者に伝送してしまう危険にさらすことになる。

4

【０００４】コンピュータシステムへの侵入者は、ネットワークを通じてコンピュータに保管されているデータを盗み出したり、データの消去、内容の書き換えなどを行う。また、内部ネットワークシステムそのものの機能を破壊し、データ通信やコンピュータを使った業務を妨害するための侵入も企てることがある。さらに、進入したコンピュータを、ある通信ネットワークを攻撃するための、前線基地として使うこともある。

【０００５】こうした危険からコンピュータを守るために、ＩＤとパスワードを使用する方法、ファイアウォールを設ける方法、情報の暗号化をする方法、デジタル署名を利用する方法、ワンタイムパスワードを使用する方法、アクセス権の制御をする方法、ウイルスワクチンを用意する方法等が利用されている。

【０００６】

【発明が解決しようとする課題】ところで、上記のような従来の技術には、次のような解決すべき課題があった。

【０００７】ユーザー名（ＩＤ）とパスワードは、不正アクセスを防止するために、コンピュータに正規の使用者であることを判別させるために使用されている。ユーザー名は宛先識別用に自由に使われる。しかし、パスワードは、本人以外は知らないということを前提として使用される。ここで侵入者がいったんユーザー名とパスワードとを盗むことに成功すると、いつでも正式な利用者に成りすまして堂々とコンピュータシステムにアクセスでき、データの盗難、改竄、破壊がいともたやすく実行できるという問題がある。

【０００８】ファイアウォールは、ネットワークの内部と外部との間にあって、情報の出入りを見張る。これは、入ってくる情報と出ていく情報の双方をチェックし、通過させてよい情報といけない情報を選択する役目を持つ。また、アクセスの全記録を残す機能を持ち、問題が発生したときの対策を講じることがでる。しかしながら、ファイアウォールも内部ＬＡＮに接続したコンピュータのひとつで、処理速度がＬＡＮ全体に影響を与える。また、チェック機能と処理速度のバランスが実用に耐えるものでなければならない。しかも、システム内部に侵入してしまったウイルス等には対応できない。

【０００９】既に開発された公開鍵、秘密鍵といった暗号化鍵を使用した方法によれば、通信中の情報の盗聴を効果的に防止することが可能である。しかしながら、鍵を盗まれないように管理が必要なこと、多数のメンバー相互間や、次々に相手が変わる不特定の相手とのやり取りには向かないという問題がある。デジタル署名も暗号化技術を発展させたもので、多数のメンバー相互間や、次々に相手が変わる不特定の相手とのやり取りには向かないという問題は解決されない。

【００１０】ワンタイムパスワードは、二度繰り返して使うことができない一度限りのパスワードである。アク

セスのたびにパスワードが変わるので、盗難にあっても、次回以降は使えないという点で、一般のパスワードより安全性は高い。しかし、用途が限定され、パスワードの管理が煩雑になるという問題がある。

【００１１】アクセス権の制御は、オペレーティングシステムに記憶装置等へのアクセスの際にパスワードの入力を要求する機能を持たせたもので、ユーザー名（ＩＤ）とパスワードを使用する方法における問題点を解決するものではない。

【００１２】ウイルス対策としてウイルスチェッカやワクチンソフトを使用する方法は、既知のコンピュータウイルスの侵入を阻止してその機能を停止させることができても、未知のコンピュータウイルスには効果がないという問題がある。すなわち、ウイルスプログラムと正常のプログラムとの区別がつかなければ感染を防止できないという問題がある。

【００１３】

【課題を解決するための手段】本発明は以上の点を解決するため次の構成を採用する。

〈構成１〉コンピュータ上で動作するアプリケーションプログラムに、重複しないユニークな識別コードを割り付けた識別コード応答モジュールを含めておくとともに、上記アプリケーションプログラムをインストールされるコンピュータ上で、上記識別コードと同一の識別コードを割り付けた識別コード認証モジュールを動作させ、この識別コード認証モジュールと上記識別コード応答モジュールの通信により識別コードの一致が確認されたときにのみ、インストーラに上記アプリケーションプログラムのインストールを実行させることを特徴とするアプリケーションプログラムのインストール管理方法。

【００１４】〈構成２〉コンピュータにダウンロードされる任意のデータ群に、重複しないユニークな識別コードを割り付けた識別コード応答モジュールを含めておくとともに、上記データ群をダウンロードされるコンピュータ上で、上記識別コードと同一の識別コードを割り付けた識別コード認証モジュールを動作させ、この識別コード認証モジュールと上記識別コード応答モジュールの通信により識別コードの一致が確認されたときにのみ、コントローラに上記データ群のダウンロードを実行させることを特徴とするデータ群のダウンロード管理方法。

【００１５】〈構成３〉予めコンピュータに登録されたアプリケーションプログラムが、予めそのコンピュータに登録された識別コードを付加したコマンドを発行した場合にのみ、そのコンピュータ上での当該コマンドの実行を許可する識別コード認証モジュールを備えたことを特徴とするコンピュータ。

【００１６】〈構成４〉構成３に記載のコンピュータにおいて、識別コード認証モジュールは、任意のタイミングで、アプリケーションプログラムに対して登録された識別コードを別の識別コードに更新することを特徴とするコンピュータ。

【００１７】〈構成５〉一定の重複しないユニークな識別コードであって、予め登録したものを付加したデータを使用したアクセスのみを許可するデータアクセス管理モジュールを備えたことを特徴とするコンピュータ。

【００１８】〈構成６〉コンピュータと所定の情報交換処理を実行する媒体に、重複しないユニークな識別コードを割り付けた識別コード応答モジュールを含めておくとともに、上記媒体を上記コンピュータに接続したとき、上記媒体に対応する識別コードをコンピュータに登録して管理する識別コード認証モジュールをコンピュータ上で動作させ、この識別コード認証モジュールと上記識別コード応答モジュールの通信により、媒体中の識別コード応答モジュールに割りつけられた識別コードと、その媒体に対応する登録された識別コードの一致が確認されたときにのみ、上記情報交換処理を実行させることを特徴とする情報交換処理の管理方法。

【００１９】〈構成７〉構成６に記載の管理方法において、識別コード認証モジュールは、情報交換処理が終了したタイミングで、上記媒体の識別コード応答モジュールを、これまでとは別のユニークな新たな識別コードを割り付けたものに更新するとともに、コンピュータにその新たな識別コードを、当該媒体に対応するものとして登録することを特徴とする情報交換処理の管理方法。

【００２０】〈構成８〉コンピュータにインストールしようとする情報が記録された記憶媒体には、認証用データをやりとりして認証処理を実行する機能を持つ応答モジュールが記録され、上記情報をインストールするコンピュータは、上記応答モジュールと認証用データをやりとりして認証処理を実行する機能を持つ認証モジュールと、認証処理が正常に終了したとき、上記記憶媒体に記憶された情報をコンピュータにインストールするインストーラとを備え、少なくとも上記認証モジュールは、ネットワークを通じて認証モジュール配信用サーバからダウンロードされることを特徴とする情報のコンピュータへのインストール方法。

【００２１】〈構成９〉構成８に記載のインストール方法において、認証モジュール配信用サーバに対して認証モジュールのダウンロードを要求する機能を持つ配信要求モジュールを備えることを特徴とする情報のコンピュータへのインストール方法。

【００２２】〈構成１０〉構成８に記載のインストール方法において、認証モジュール配信用サーバには、認証モジュールの配信履歴データを記録する配信記録部が備えられていることを特徴とする情報のコンピュータへのインストール方法。

【００２３】〈構成１１〉構成８に記載のインストール方法において、認証モジュールは、コンピュータに正常に情報のインストールが終了すると無効化されることを特徴とする情報のコンピュータへのインストール方法。

【００２４】〈構成１２〉カードを使用して自動的に所定の取引を実行する自動取引装置において、上記カードには、入力データを所定のアルゴリズムで変換して識別コードを発生する第１の識別コード発生モジュールと、この第１の識別コード発生モジュールの出力する識別コードを保持して、次のタイミングで、保持していた識別コードを上記第１の識別コード発生モジュールに入力する第１の識別コードレジスタとが設けられ、上記ＡＴＭには、入力データを上記第１の識別コード発生モジュールと同一のアルゴリズムで変換して識別コードを発生する第２の識別コード発生モジュールと、この第２の識別コード発生モジュールの出力する識別コードを保持して、次のタイミングで、保持していた識別コードを上記第２の識別コード発生モジュールに入力する第２の識別コードレジスタと、上記第１の識別コード発生モジュールの出力した識別コードと上記第２の識別コード発生モジュールの出力した識別コードとが一致したかどうかを判定して認証処理をする認証モジュールが設けられ定ることを特徴とする自動取引装置の認証処理方法。

【００２５】〈構成１３〉構成１２に記載の自動取引装置の認証方法において、上記第１の識別コード発生モジュールは、認証処理開始直前に入力されたパスワードと第１の認証コードレジスタに保持された認証コードを受け入れて、新たな認証コードを発生し、上記第２の識別コード発生モジュールは、認証処理開始直前に入力されたパスワードと第２の認証コードレジスタに保持された認証コードを受け入れて、新たな認証コードを発生することを特徴とする自動取引装置の認証処理方法。

【００２６】〈構成１４〉コンピュータに設けられた監視モジュールであって、予め管理テーブルに認証コードが登録されたアプリケーションによる要求のみをオペレーティングシステムに伝えるように動作し、ネットワークに接続されたネットワークインターフェイスを通じて、予め特定された記憶領域にデータが書き込まれる処理は前記監視モジュールの監視外に置くように、コンピュータを動作させるコンピュータプログラム。

【００２７】

【発明の実施の形態】以下、本発明の実施の形態を具体例を用いて説明する。図１は本発明のプログラムやデータの管理方法を実施するためのシステムブロック図である。図のネットワーク１には、アプリケーションプログラムやネット配信データの供給元３のコンピュータやサーバが接続されている。また、ネットワーク１には任意のクライアントの端末５が接続されている。この端末５は、パーソナルコンピュータやモバイルコンピュータその他様々な任意のコンピュータである。ネットワーク１はデータやプログラムを転送できるものであればなんでもよいが、例えば、インターネットやイントラネットなどのネットワークである。このようなシステムでは、端末５はネットワーク１を通じてアプリケーションプログラムやネット配信データを取得することができる。

【００２８】しかしながら、こうしたシステムを利用すれば、ダウンロードされたアプリケーションプログラムやネット配信データをそのまま別の端末に転送し、別の端末で不正使用することが可能になる。すなわち、そのまま使用できるような状態でアプリケーションプログラムやデータをネットワーク１を通じて配信すると、供給元は、プログラムやデータの著作権を確実に守ることか難しいという問題があった。

【００２９】この発明では、アプリケーションプログラムやデータを端末５にダウンロードしても、そのままでは使用できないようにする。またあるいは、正規の許可を得ない限り、ダウンロードができないようにする。このために、例えば、識別コード発行センター６を設ける。この識別コード発行センター６は、アプリケーションプログラム供給元３から供給される全てのアプリケーションプログラムに対し、互いに重複しないユニークな識別コードを割り付ける。そして、その識別コードをキーとして応答する識別コード応答モジュール７をアプリケーションプログラム供給元３に対して提供する。

【００３０】この識別コード応答モジュール７は、アプリケーションプログラムに組み込まれる。識別コード応答モジュール７は、例えば、問い合わせコマンドに割りつけられた識別コードを付加して問い合わせをすると、「ＧＯＯＤ」という意味の応答を出力し、その他の場合には、「ＮＧ」という意味の応答を出力するように機能するコンピュータプログラムである。識別コード応答モジュール７は、割りつけられた識別コードを表示する機能を持つものであれば、何でも良いが、アプリケーションプログラム側から識別コードを出力させないようにしたほうが、不正コピーの防止にはより効果的である。

【００３１】さらに識別コード発行センター６は、クライアントの端末５がアプリケーションプログラムのダウンロードを要求するとき、上記の識別コード応答モジュールと同一の識別コードを割り付けられた識別コード認証モジュールを供給クライアント側に供給する。クライアントは、例えば、予めアプリケーションプログラムの購入契約をして、識別コード認証モジュールの供給を受ける権利を獲得する。識別コード発行センター６は、識別コード認証モジュール８をネットワーク１を通じて端末５に送信する。この識別コード認証モジュール８は、端末５の所定の記憶領域書き込まれて、ダウンロードされたアプリケーションプログラムをインストールする際に、後で説明する認証処理を実行する。

【００３２】この識別コード認証モジュール８を端末５に送り込む方法は、識別コード発行センター６がネットワーク１を通じて直接端末５に転送する以外にもある。例えば、アプリケーションプログラム供給元３が、識別コード発行センター６から供給された識別コード認証モジュール８を、ネットワーク１を通じて端末５に送り込

む方法がある。ただし、アプリケーションプログラムとは別の方法で別のタイミングで送り込むようにしないと、アプリケーションプログラムとは別に識別コード認証モジュール８を用意して配布する効果が小さくなる。アプリケーションプログラムと識別コード認証モジュール８とを一緒にコピーすれば、不正コピーが可能になるからである。従って、例えば、アプリケーションプログラムの購入契約成立時に、クライアントが意識しない状態で、クライアントの端末に識別コード認証モジュール８をダウンロードするようにすることが好ましい。

【００３３】また、上記の例では、ネットワーク１を通じてアプリケーションプログラムをクライアントの端末にダウンロードする例を示して説明をしたが、アプリケーションプログラムがＣＤ－ＲＯＭ１５などの媒体に記録されていたとしても同様の処理が可能である。この場合には、必ず、識別コード認証モジュール８を全く別のルートで端末５に送り込むようにする。

【００３４】端末５にアプリケーションプログラムがダウンロードされ、インストールを開始すると、図１に示した１点鎖線の中に示すようなプログラムやモジュールが、端末５上で起動される。アプリケーションプログラム識別コード応答モジュール１１は、ダウンロードされたアプリケーションプログラムのものである。インストーラ１２は、アプリケーションプログラムをインストールして使用可能にするためのセットアップ制御を行うプログラムである。識別コード認証モジュール１３は、識別コード発行センター６から端末５に対して供給を受けたプログラムモジュールである。

【００３５】図２は、上記のアプリケーションプログラム識別コード応答モジュール１１とインストーラ１２と識別コード認証モジュール１３の動作を示すシーケンスチャートである。このシーケンスが開始される前に、予め、図１に示す端末５に対しアプリケーションプログラムがダウンロードされ、さらに識別コード認証モジュール８が端末５の所定の記憶領域上に記憶されているものとする。ここで、アプリケーションプログラムのセットアップのためにインストーラ１２を起動する（ステップＳ１）。このときインストーラ１２は、識別コード認証モジュール１３に対し、認証依頼を行う（ステップＳ２）。識別コード認証モジュール１３は、ステップＳ３において認証用の識別コードを発生する（ステップＳ３）。この識別コードは、ダウンロードされたアプリケーションプログラムの識別コード応答モジュール７に割り付けられたものと同一のものである。

【００３６】識別コード認証モジュール１３は、発生させた識別コードを付加した問い合わせコマンドを識別コード応答モジュール１１に対して送信する（ステップＳ４）。識別コード応答モジュール１１は、この識別コードのチェックを行う（ステップＳ５）。自分に割り付けられた識別コードと同一の識別コードを付加した問い合わせコマンドが入力した場合には、識別コードが一致したという応答を行う。また、それ以外の場合には、識別コードが不一致であるという応答を行う。ステップＳ６でこのような応答があると、識別コード認証モジュール１３は、識別コードが一致したときにはステップＳ７からステップＳ８に進み、インストーラ１２に対し、インストールの続行指示をする。それ以外の場合には、ステップＳ１２でエラー処理を行なう。

【００３７】識別コード認証モジュール１３からインストールの続行指示がインストーラ１２に送られると、インストーラ１２では、ダウンロードされたプログラムのインストールを実行する（ステップＳ９）。こうしてプログラムのインストールが完了する。インストールが完了すると、インストーラ１２は、識別コード認証モジュール１３に対し、インストール処理の完了通知を送る（ステップＳ１０）。識別コード認証モジュール１３は、その後のアプリケーションプログラムの実行監視のために、アプリケーション管理テーブルを生成する（ステップＳ１１）。このアプリケーション管理テーブルは、図１に示した端末５の所定の不揮発性メモリに記録され、アプリケーションプログラムが動作するときに、後で説明するような要領で動作管理を行う。

【００３８】上記の方法によれば、図１に示すアプリケーションプログラム供給元３から端末５に対してダウンロードされたアプリケーションプログラムを、そのまま別のコンピュータにコピーしたとしても、識別コード認証モジュールが動作しないため、インストールをしてセットアップをすることができない。すなわち正式にプログラムの購入契約をしたクライアント以外はアプリケーションプログラムのインストールができないので、不正コピーを防止できる。なお、上記の方法によって管理できるのはアプリケーションプログラムに限らない。ネットワークを通じて配信される様々なデータ、例えば、音楽データ、書籍データなどについても同様のことが言える。もちろん、他の媒体例えば、フロッピー（登録商標）ディスクやＣＤ－ＲＯＭやメモリカードによって配布される任意のデータについても同様である。これらのデータは予め所定の識別コード応答モジュールを組み込んで配信されるようにしておく。識別コード認証モジュール８は、実際にそのデータを使用する権利を、例えば有償で獲得したクライアントの端末に、別ルートで供給する。これで、アプリケーションプログラムの不正コピーなどを防止することが可能になる。

【００３９】また、例えば、予め所定の識別コードを割り付けたプログラムやデータや各種著作物を記憶させたＣＤ－ＲＯＭをダイレクトメールや雑誌の付録などによって提供する。しかしながら、インストール処理を実行しなければ、これらは利用できないようにしておく。その状態は、図１に示す端末５にアプリケーションプログラムやデータがダウンロードされたのと同様の状態であ

る。ここで、クライアントの端末５のユーザーが、ネットワーク１を通じて、例えばそのＣＤ－ＲＯＭのシリアル番号などとＣＤ－ＲＯＭに記録された自分の利用したいプログラムの名称などをアプリケーションプログラム供給元３に通知する。そこで代金の決済が終了すれば、そのＣＤ－ＲＯＭのシリアル番号基づいて、ＣＤ－ＲＯＭに記録したアプリケーションプログラムに割り付けられた識別コードを調べて、対応する識別コード認証モジュールを、クライアントの端末５に送る。

【００４０】これで図２に示した通りの処理が可能になる。さらに、上記の例では、識別データを利用して、コンピュータにコピーされ、あるいはダウンロードされたプログラムやデータの使用を可能にするかどうかの管理をしたが、コンピュータにコピーやダウンロードを許可するかどうかの管理を行なうようにしてもよい。

【００４１】上記の識別コードは、識別コード発行センターでなく、アプリケーションプログラムの供給元で発行することも可能である。しかしながら、いかなる場所いかなる環境においても重複しない識別コードが利用されることがこのシステムの安全な運用に結びつく。従って、識別コード発行センター６を設け、全てのアプリケーション供給元や音楽配信会社などが、この識別コード発行センター６に識別コードの発行を依頼するようなシステムが好ましい。こうすれば、常にユニークな識別番号を継続的に発行し、信頼性の高い管理が可能になる。

【００４２】なお、識別コード認証モジュール８をコンピュータから取り出してダウンロードされたアプリケーションプログラムと共にコピーすれば、アプリケーションプログラムの不正コピーが可能になる。そこで、例えば識別コード認証モジュールは一度インストールを実行した後は、例えばインストーラ１２によって削除されるという方法も採用できる。これによってアプリケーションプログラムのインストールを１回だけに制限することが可能になる。アプリケーションプログラムの修復などについては、ネットワークを通じて供給元が充分なサポートをすればよい。

【００４３】図３の（ａ）は、コンピュータにインストールされたアプリケーションプログラムの動作を制限してセキュリティを高める管理方法の説明図で、（ｂ）はその動作フローチャートである。図２のステップＳ１１でアプリケーションプログラムのインストールが終了すると、識別コード認証モジュール１３がコンピュータ中にアプリケーション管理テーブルを生成するようにした。アプリケーション管理テーブルは、図３に示すように、アプリケーションの名称２７と識別コード２８とを対応付けたものである。この識別コード２８は、アプリケーションプログラムのインストールをする際に使用した識別コードとは全く異なるものであってよい。この例では、インストールされたアプリケーションプログラム２１は、動作をする際に発行するコマンド２２に、常に一定の識別コード２３を付加する。コマンド２２はＯＳ（オペレーティングシステム）に送り込まれる際に、まず、シェル２４の部分で解釈され、その解釈の結果がカーネル２５に転送される。

【００４４】このシェル２４でコマンド２２を解析する際に、どのアプリケーションプログラムから発行されたコマンドかを判断する。同時に付加された識別コードを取得する。そして、アプリケーション管理テーブル２６を参照し、そのアプリケーションプログラムがどの識別コードを付加してコマンドを発生するかを調べる。シェル２４は、アプリケーションプログラム２１が、アプリケーション管理テーブル２６に登録された通りの識別コード２８をコマンド２２に付加して発行した場合にのみ、コマンド２２を解釈して、カーネル２５に転送するようにする。正規の手順を経ないでインストールされたアプリケーションプログラムは、アプリケーション管理テーブル２６に登録されない。また、ネットワーク等を通じてコンピュータに侵入した不正なコマンドは必要な識別コードが付加されていない。従って、そのコマンドはシェルにより処理を拒絶され、ＯＳに転送されないから、実行されることがない。すなわち、特定の登録されたアプリケーションプログラム以外はそのコンピュータ上で全く動作しないという環境が設定できる。従って、極めて安全性の高いシステムが確立される。

【００４５】図３の（ｂ）を用いて、具体的なコマンド解釈動作を説明する。まず、シェル２４がステップＳ２１でいずれかのアプリケーションプログラムからコマンドを受け付ける。ステップＳ２２では、アプリケーション管理テーブル２６を参照して、コマンド２２に付加された識別コード２３が、登録されたアプリケーションプログラム２１の識別コード２８と一致するかどうかを判断する。一致すれば、ステップＳ２３に進み、コマンドの処理を実行する。一致しなければ、ステップＳ２４に進み、エラー処理を実行し、そのコマンドの処理を拒絶する。なお、この例では、あらゆるコマンドは、シェル２４でのみ受け付けられて、シェル２４でのみ解釈されるという手順を確立しておくとよい。これで、極めてセキュリティの高いコンピュータシステムが確立できる。

【００４６】図４の（ａ）はデータアクセスのセキュリティを高めるための管理方法を実現したシステムのブロック図であり、（ｂ）はその動作フローチャートである。この実施例では、コンピュータで使用されるあらゆるメモリ、あるいは、保護を必用とするメモリ領域、例えば、特定のドライブに対するデータアクセスに上記の識別コードを利用する。図に示すように、データアクセス管理モジュール３１は、メモリ３２に記憶されたデータ３３や、メモリ３２に書き込まれるこれ以外のデータについてのアクセス管理を行う。このためにメモリ管理テーブル３４を利用する。アクセスに利用されるデータは、図に示すように、アクセスコマンド３５とデータ３

６と識別コード３７とから構成される。メモリ管理テーブル３４には、例えばアクセス管理をされるドライブ名３８と識別コード３９とを対応させて記憶させておく。この実施例では、メモリ管理テーブル３４に登録されたドライブには、該当する識別コードを付加したデータしか読み書きできないようにする。

【００４７】すなわち、アクセスコマンド３５とデータ３６と識別コード３７とがデータアクセス管理モジュール３１に入力すると、図の（ｂ）に示すように、まずステップＳ３１でそのコマンドを受け付ける。ステップＳ３２で、データアクセス管理モジュール３１は、メモリ管理テーブル３４を参照する。そしてアクセスの対象がドライブ３８であると判断すると、登録された識別コード３９と、データ３６に付加された識別コード３７とを比較し、両者が一致するか判断する（ステップＳ３２）。両者が一致すればメモリ３２をアクセスするコマンドの実行を許可し、例えばデータの書き込みなどを許す（ステップＳ３３）。一方、識別コードが一致しない場合には、ステップＳ３０に進み、エラー処理を実行する。すなわち、データのアクセスを受け付けない。このデータアクセス管理モジュール３１は、例えば、図３を用いて説明したシェルの一部の機能モジュールであってもよいし、全く独立に設けられたプログラムモジュールであってもよい。

【００４８】以上のようにすれば、データに予め登録された識別コードが付加されていない場合には、該当するドライブのアクセスをすることができない。該当するドライブのデータを読み出すこともできないし、書き込むこともできない。従って、識別コードの管理を厳重にしておけば、ドライブ２はその識別コードを付加してアクセスをするアプリケーション以外のアクセスが完全に阻止される。従って、例えばネットワークを通じてコンピュータ中に入り込んだデータがメモリ上に無断で書き込まれるおそれがなく、極めてセキュリティの高いシステムを確立できる。

【００４９】図５の（ａ）は上記のシステムをキャッシュカードなどに利用した管理方法の説明図で、（ｂ）はその動作フローチャートである。図５において、カード４１は、ＩＣカードと呼ばれるキャッシュカードやクレジットカードであって、メモリを内蔵したカードである。このメモリに、既に説明したような所定の識別コードを割り付けられた識別コード応答モジュール４２が記憶される。ＡＴＭ（自動現金取引装置）４３には、既に説明したような機能を持つ識別コード認証モジュール４４が記憶されている。

【００５０】このＡＴＭ４３は、例えば銀行などの窓口において預貯金の入出金に利用されている良く知られた装置である。図示しない多数のＡＴＭ４３は、いずれも、金融システムを管理するホストコンピュータ４０と接続されている。なお、クレジットカードの場合には、クレジットカード読み取り装置などがこのＡＴＭの代わりに利用される。カード４１をＡＴＭ４３に装着すると、所定の手順によって認証処理がされ、よく知られた現金の入出金処理が実行される。このとき、上記識別コード応答モジュール４２と識別コード認証モジュール４４との間で、識別コードの認証処理が行われる。まず、カード４１をＡＴＭ４３に装着すると（ステップＳ４１）、カード４１の利用者や口座番号などが、カードのメモリ中から自動的にＡＴＭ４３に読み取られる。ＡＴＭ４３の側では、ホストコンピュータ４０の顧客管理用データベースを参照して、その利用者の識別コードに該当するデータを取得する。

【００５１】識別コード認証モジュール４４は、その識別コードを付加した問い合わせコマンドを出力して、カード４１の識別コード応答モジュール４２に問い合わせを行う。識別コードが一致している場合には、真正なカードであると判定され、認証が終了し（ステップＳ４２）、カードの取引が実行される（ステップＳ４３）。この処理の基本的な手順は既に図１のシステムの動作で説明したのと同様である。カード４１にこのような機能を持たせると、識別コード応答モジュール４２自体は、識別コードを発生させないため、カード４１を調べても、ユーザーの識別コードを盗むことができない。

【００５２】さらにこの実施例では、次のような手順によってカードを１回利用するたびに識別コードが変更されるように制御する。すなわち、カード４１をＡＴＭ４３に装着して１回の取引を終了すると、ＡＴＭ４３は、新たな識別コード応答モジュールをカード４１に書き込む。すなわち、カード４１に当初記憶されていた識別コード応答モジュール４２に代えて、これとは異なる別の識別コード応答モジュール４５がカード４１に記憶される（ステップＳ４４、４５）。当初の識別コード応答モジュール４２には識別コードＸが割り付けられていたとする。この場合に取引が終了すると、カード４１には、別の識別コードＹが割り付けられた識別コード応答モジュール４５が記憶される。ＡＴＭ４３の側では、識別コードをＸからＹに変更した旨を登録する。すなわち、次にこのカード４１の利用者がＡＴＭを使用する場合には、識別コードＹで認証処理が行われることになる。

【００５３】上記のようにすれば、当初からカード４１の中には、識別コードを直接読み取ることができるようなデータは、記録されていないから、カードをそのままコピーしない限り、そのカードを偽造できない。例えば、識別コード応答モジュール４２は、識別コードを付加された問い合わせコマンドを受け入れたときに自分に割り付けられた識別コードと一致するかどうかを判断して、イエスあるいはノーという応答をするコンピュータプログラムである。従って、単純に外からデータを解析しても直接識別コードを読み取ることができないので、本人の識別コードを厳重に秘密に管理することができる

という効果がある。さらに、取引の都度識別コードが切り替えられるという方法を採用すれば、万一カード４１の識別コード応答モジュール４２をコピーして別のカードを用いてＡＴＭを操作しようとしても、そのときには識別コードが切り替わってしまっていて使用できない。故に、不正にコピーをしたカードは全く使用不能になる。すなわち、暗証番号を盗んだり、カードを不正にコピーしたものの使用を完全に阻止することが可能になる。

【００５４】取引のたびにカードに新たな識別コードが割り付けられて、これまでの識別コードは無効になるという管理方法を採用する場合には、重複しないユニークな識別コードを発生する機構が必要になる。もちろん、利用者の利用者コードと組み合わせて使用されるのだから、完全に唯一無二の識別コードでなければならないというわけではない。例えば、国とか地域内ではユニークであるものとか、例えば、１０年位の期間は重複が発生しないものというようにして識別コードを発生させてもよい。金融システムの場合、ホストコンピュータ４０の部分にこうした識別コード発行機構を設けておき、ホストコンピュータ４０によって管理される全てのＡＴＭに対しユニークな識別コードを供給するというシステムを組むことが好ましい。また、ホストコンピュータ４０では常にどのユーザーがどの識別コードを使用しているかを管理し、切り替わっていく識別コードに応じて取引を実行できるようにするとよい。

【００５５】また、図５の方法を図３や図４のコマンドに付加する識別コードに採用してもよい。例えば、アプリケーションプログラムが動作を開始するときに使用した識別コードは、動作が終了すると新たなものに更新される。同時にアプリケーション管理テーブルも書き換えられる。データのアクセス時に使用した識別コードは、一連のアクセス処理が終了すると新たなものに更新される。同時にメモリ管理テーブルも書き換えられる。識別コード応答モジュールを生成する識別コード認証モジュールが常にアプリケーションプログラムの動作やデータのアクセスを管理して、タイミングよく識別コードを更新していけば、きわめてセキュリティの高いプログラムやデータ管理が可能になる。

【００５６】図６は本発明の変形例のブロック図である。図３の実施例では、シェル２４がアプリケーション管理テーブルを参照して、登録された識別コードを付加しないコマンドの解釈を拒絶してオペレーティングシステムを保護した。図６の例では、この種の機能をカーネル側に持たせる。図６ではＵＮＩＸ（登録商標）のオペレーティングシステムのシステムコールインタフェース６１がアプリケーション管理テーブル５６を参照する。即ち、アプリケーションプログラム２１やライブラリ群５１から識別コードを付加したコマンドがカーネル６０のシステムコールインタフェース６１に受けつけられる。システムコールインタフェース６１は、アプリケーション管理テーブル５６を参照する。アプリケーション管理テーブル５６は、アプリケーションプログラム２１やライブラリ群５１の名称５７と、それらの使用する識別コード５８と対応させて登録したものである。システムコールインタフェース６１はアプリケーションプログラム２１やライブラリ群５１が登録された識別コードを使用した場合は、コマンドをファイルサブシステム６２やプロセス制御サブシステム６３に伝え、それ以外の場合はエラー処理をするように制御する。これにより、図３の例と同様の管理が可能になる。図３のケースでも図６のケースでも、オペレーティングシステムにコマンドが達する前に識別コードをチェックして、不正なコマンドのオペレーティングシステムへの進入を阻止する事が出来る。即ち、オペレーティングシステムへ達する全てのコマンドの正当性を、そのコマンドに付加された識別コードを利用して判定する手段をコンピュータ中のいずれかの場所に設ければ、不正なコマンドのオペレーティングシステムへの進入を完全に阻止する管理が可能になる。もちろん、重要な機能を持つ特定のコマンドにのみ識別コードを付加するというルールを採用して、識別コードチェックの負荷を低減してもかまわない。

【００５７】図７は、これまでとは別の管理方法の実施例で、プログラムやデータの不正コピー防止機能を強化したものの説明図である。図のＣＤ－ＲＯＭ７０は、コンピュータプログラムや音楽その他様々なデータであって、コンピュータにインストールしようとする情報が記録された記憶媒体である。これらのデータをコンピュータ８５にダウンロードしたり、インストールしたりする場合の、不正コピーを防止する。このために、ＣＤ－ＲＯＭ７０に、データ７１とともに、応答モジュール７２を記録しておく。データ７１は、例えば、音楽とかコンピュータプログラムを、よく知られた圧縮形式で格納したものである。応答モジュール７２は、認証モジュール７３と暗証コード等の認証用データをやりとりする機能を持つコンピュータプログラムである。この認証手順は既に説明をした。

【００５８】コンピュータ側には、認証モジュール７３と解凍モジュール７４とインストーラ７５が動作できる状態で準備されている。解凍モジュール７４は、圧縮処理されたデータ７１を解凍処理する機能を持つプログラムである。インストローラ７５は解凍されたデータをコンピュータ８５の指定された部分に転送して記録する、良く知られたインストール処理を実行する機能を持つプログラムである。認証モジュール７３は、ネットワーク８０を通じてコンピュータ８５に取り込まれる。このために、コンピュータ８５には、配信要求モジュール８１を設けておく。配信要求モジュール８１は、認証モジュール配信用サーバ７７に対して、例えば、対話式で認証モジュールのダウンロードを要求する機能を持つコンピ

ュータプログラムである。また、ネットワーク８０に接続された認証モジュール配信用サーバ７７には、どの利用者にどのような認証モジュールをいつ送信したかといった、認証モジュールの配信履歴データを記録する配信記録部７６を設けておく。配信記録部７６は、認証モジュール配信用サーバ７７に接続された記憶装置などからなる。

【００５９】このシステムでは、市販されたり、各種の方法で配布されるＣＤ―ＲＯＭ７０だけを使って、コンピュータ８５にデータやコンピュータプログラムをインストールすることができない。利用者は、あらかじめ一定の契約をして、配信要求モジュール８１を操作して、認証モジュール配信用サーバ７７に認証モジュール７３の配信要求をし、コンピュータ８５にダウンロードしておかなければならない。この認証モジュールが、ＣＤ―ＲＯＭ７０に記録されたデータ７１のインストールを制御する。

【００６０】この実施例では、正常にデータ７１のインストールが終了すると、認証モジュール７３はすみやかに無効化される。すなわち認証モジュール７３を使用したインストール処理を、１回だけしかできないようにする。これにより認証モジュール７３を盗み出してＣＤ―ＲＯＭ７０に記録されたデータの不正コピーをする行為などを防止できる。なお、インストール後に何らかの障害が発生して、ＣＤ－ＲＯＭにより正規の利用者がデータ７１の再インストールをしようとした時には、速やかに認証モジュール７３を再配信できる体制が必要になる。そこで、配信要求モジュール８１をコンピュータ８５に残しておき、いつでも認証モジュール配信用サーバ７７に配信を要求できるようにする。この場合に、認証モジュール７３の配信履歴を配信記録部７６に記録しておく。この配信記録は、利用者の認証モジュール７３の不正利用を抑制する機能を持つ。認証モジュール７３を要求できるのは、契約した利用者のみであるから、そのインストール先やインストールされたデータの管理と全てのインストール作業に、利用者が明確な責任を持つことになる。従って、利用者の知らない間に利用者のＣＤ－ＲＯＭを不正にコピーしてデータやコンピュータプログラムをインストールするという問題が無くなる。

【００６１】図８は、図７に示したシステムの具体的な動作フローチャートである。まず（ａ）に示すようにして、利用者は認証モジュールの配信を受ける。ステップＳ４６において配信要求モジュール８１が起動すると、認証モジュール配信用サーバ７７が配信要求を受け付ける。次にステップＳ４７において、配信記録部７６の記録を更新する。そしてステップＳ４８において認証モジュール配信用サーバ７７は、認証モジュール７３をネットワーク８０を通じて利用者の端末に配信する。こうして認証モジュール７３が利用者の端末上で起動できる状態になると、（ｂ）に示すインストール処理が実行される。

【００６２】はじめにステップＳ５１において認証モジュールがダウンロードされると、ステップＳ５２でインストール処理を開始する。ＣＤ－ＲＯＭ７０の応答モジュール７２がコンピュータ８５に転送されて起動し、認証モジュール７３と暗証コードなどをやりとりして認証処理を実行する。認証をパスしない場合にはエラーが発生する。認証をパスするとステップＳ５４に進む。そして解凍モジュール７４がＣＤ－ＲＯＭ７０に記録されたデータ７１の解凍を行う。ステップＳ５５では、インストローラ７５がインストール処理を実行する。正常にインストールが終了すると、ステップＳ５６において認証モジュール７３の無効化が行われる。認証モジュール７３の無効化方法は自由である。認証モジュール自身を消去する方法の他、認証モジュール７３を動作させるためのパラメータを消去するといった方法も可能である。

【００６３】図９は、銀行のキャッシュカードなどに本発明の方法を利用した場合の変形例説明図である。図の（ａ）はカードとＡＴＭ（現金自動取引装置）の主要部ブロック図、（ｂ）はその動作説明図である。（ａ）に示すように、カード側には識別コード発生モジュール９０と識別コードレジスタ９１が設けられている。識別コード発生モジュール９０は、カードに搭載されたコンピュータ上で動作するコンピュータプログラムである。識別コードレジスタ９１はカードのメモリ中の記憶領域に設けられる。また、ＡＴＭ側にも同じように識別コード発生モジュール９５と識別コードレジスタ９６が設けられている。識別コード発生モジュール９５は、ＡＴＭのコンピュータ上で動作するコンピュータプログラムである。識別コードレジスタ９６はＡＴＭのメモリ中の記憶領域に設けられる。

【００６４】識別コード発生モジュール９０は、認証処理開始直前にパスワード９２を入力すると、認証モジュール９９が処理を開始する前に、識別コードレジスタ９１に記憶された識別コードを読み出して、新たな識別コードを発生する機能を持つ。識別コード発生モジュール９５も全く同様の機能を持ち、パスワード９２が入力した時に、識別コードレジスタ９６に記憶された識別コードを利用して新たな識別コードを発生する。識別コード発生モジュール９０と識別コード発生モジュール９５の機能は全く同一であって、同一のパスワードと同一の識別コードを入力すると、同一の新たな識別コードを発生する。従って、この図に示すような状態で、顧客がＡＴＭにカードを装着してパスワード９２を入力すると、カード側とＡＴＭ側で同時に新たな識別コードを発生させる。このとき、カード側とＡＴＭ側で全く同一の識別コードが得られる。これが認証モジュール９９で比較され、認証処理が行われる。すなわち、カード側で識別コード発生モジュール９０が発生した識別コードとＡＴＭ側で識別コード発生モジュール９５が発生した識別コー

ドとが一致すれば、認証処理が正常に終了したとして現金の取引などが進められる。その他の場合には、エラー処理が行われる。

【００６５】この実施例では次のような非常に重要な効果が得られる。まず、カード側もＡＴＭ側も、識別コードレジスタ９１と９６に、前回使用された識別コードを記憶しているものの、次の取引に使用する識別コードはどこにも記憶していない。次の取引では、識別コードレジスタ９１と９６に記憶された識別コードと利用者の入力したパスワードを用いて生成した新たな識別コードが、認証に利用される。このため例えば、カード側に記録された情報を盗み取った第３者が識別コードレジスタ９１に記憶された識別コードを使用して不正な取引を行おうとしても、ＡＴＭは反応しない。識別コード発生モジュール９０を実際に動作させなければ、取引に必要な識別コードが得られない。

【００６６】しかも、カードを１回使うたびに、即ち、１回の認証処理ごとに全く新たな識別コードを発生させて利用するので、第３者が識別コードを直接コピーして使用することができない。新たな識別コードを発生させるのに、直前の認証処理で発生させた識別コードだけでなく、ユーザの入力するパスワードも利用するようにすれば、よりセキュリティの高い運用ができる。また、図の（ｂ）に示すように、カード１０１とまったく同一の構成のカードを第３者が製造したとする。このとき識別コードもカード１０１からカード１０２にコピーしたとする。この状態で、利用者のパスワードも盗んで第３者がすぐにカードを使用するとそのカードで有効な取引ができる。

【００６７】しかし、正規の利用者がカード１０１を使用してＡＴＭ１００を動作させると、その時点で識別コードレジスタ９１、９６に記憶された識別コードの内容が変化してしまう。すなわち１回目、２回目、３回目というようにどんどん識別コードの内容が変化してしまう。従って、以前に識別コードを不正に入手した第３者がその後カード１０２を使用しても、その時点では既に識別コードが変化しており、カード１０２は使用できない。このように単に識別コードを毎回切り換えるといった処理を行うだけでなく、上記のようにカード側とＡＴＭ側とでそれぞれ新たな識別コードを発生するモジュールを設け、新たな識別コードをその都度利用して認証処理を行うと、極めて安全性の高い取引ができる。

【００６８】図１０は、図９に示したカードを使用したＡＴＭの動作を説明するためのフローチャートである。まず、ステップＳ６１において、ＡＴＭ１００にカード１０１が挿入されると、ステップＳ６２でパスワードの入力が要求される。パスワードが入力されると、カード側とＡＴＭ側とでそれぞれ識別コード発生モジュールが起動する。カード側ではステップＳ６３で旧識別コードが読み取られ、ステップＳ６４で新たな識別コードが発生する。またＡＴＭ側でも同じようにステップＳ６５において旧識別コードが読み取られ、ステップＳ６６で新識別コードが発生する。その後ステップＳ６７で、カード側で発生した識別コードとＡＴＭ側で発生した識別コードとの比較処理を行う。この処理は、ＡＴＭ内で動作する認証モジュール９９が実行する。ステップＳ６８で両識別コードが一致したと判断すると、ステップＳ６９に進み、取引を開始する。また、一致しなかった場合には、カードは返却し、エラー処理を行う（ステップＳ７０）。

【００６９】図１１は、本発明の方法をコンピュータのオペレーティングシステムに使用した場合の別の実施例を示すブロック図である。既に説明したように、コンピュータのオペレーティングシステム１１１に任意のアプリケーション１１０をインストールし、これを動作させる場合に、管理テーブル１１３を用意して、アプリケーション１１４に対応する識別コード１１５を登録しておけば、未登録のアプリケーションがオペレーティングシステム１１１上で動作するのを禁止できる。即ち、正規に登録されたアプリケーションのコマンドのみをオペレーティングシステム１１１に渡すようにする。これにより、オペレーティングシステム１１１が全く管理していないアプリケーションからのデータ書き込み等の処理を排除し、コンピュータの正常動作を確保する。また、不正に外部からアクセスされたり、コンピュータウィルスにより不正な処理が行われるのを排除できる。

【００７０】このような厳格な管理は、限定されたアプリケーションしか使用しない、例えば、銀行などのシステムに適する。しかしながら、個人用のパーソナルコンピュータのように、インターネットに接続して様々なデータを利用し、かつ安全にアプリケーションプログラムを使用したいといった環境には不向きである。図の（ｂ）に示すものは、（ａ）に示すものを改良した例を示す。図に示すように、監視モジュール１１７は、（ｂ）に示したものと同様に、アプリケーション１１８とオペレーティングシステム１１９との間に介在する。しかしながらネットワーク２００に接続されたネットワークインターフェイス２０１の動作は、この監視モジュール１１７の監視外に置く。そして、記憶領域２０２に対しては、ネットワークインターフェイス２０１が自由にデータの書き込みなどを行えるようにする。なお、不正なデータやプログラムがメモリの任意の領域に書き込まれるのを防止するために、ネットワークインターフェイス２０１がデータを書き込むことのできる記憶領域を限定しておいても構わない。

【００７１】こうして、ネットワーク２００と接続をして一定の処理を行うための領域２０２を、監視モジュールの管理外におく。従って、例えば、ブラウザとその閲覧履歴を記憶するテンポラリファイルと、ＨＴＭＬプロトコル上で動作するアプリケーションの動作には制約を

加えない。一方、例えば、ネットワーク２００を通じてデータやアプリケーションプログラムをダウンロードして、オペレーティングシステム１１９により動作させようとする場合には、認証登録モジュール２０３が領域２０２から必要なデータを取り込み、管理テーブル１１３に登録する。この実施例によって、ネットワークと自由に通信を行い、自由にデータを取り込み、自由にアプリケーションをダウンロードする環境が得られる。

【００７２】なお、各図に示した各機能ブロックは、それぞれ別々のプログラムモジュールにより構成してもよいし、一体化したプログラムモジュールにより構成してもよい。また、これらの機能ブロックの全部または一部を論理回路によるハードウエアで構成しても構わない。また、各プログラムモジュールは、既存のアプリケーションプログラムに組み込んで動作させてもよいし、独立のプログラムとして動作させてもよい。上記のような本発明を実現するためのコンピュータプログラムは、例えばＣＤ－ＲＯＭのようなコンピュータで読み取り可能な記録媒体に記録して、インストールして利用することができる。また、ネットワークを通じてコンピュータのメモリ中にダウンロードして利用することもできる。

【図面の簡単な説明】

【図１】本発明のプログラムやデータの管理方法を実施するためのシステムブロック図である。

【図２】上記のアプリケーションプログラム識別コード応答モジュール１１とインストーラ１２と識別コード認証モジュール１３の動作を示すシーケンスチャートである。

【図３】（ａ）は、コンピュータにインストールされたアプリケーションプログラムの動作を制限してセキュリティを高める管理方法の説明図で、（ｂ）はその動作フローチャートである。

【図４】（ａ）はデータアクセスのセキュリティを高めるための管理方法を実現したシステムのブロック図であり、（ｂ）はその動作フローチャートである。

【図５】（ａ）は上記のシステムをキャッシュカードなどに利用した管理方法の説明図で、（ｂ）はその動作フローチャートである。

【図６】本発明の変形例のブロック図である。

【図７】これまでとは別の管理方法の実施例で、プログラムやデータの不正コピー防止機能を強化したものの説明図である。

【図８】図７に示したシステムの具体的な動作フローチャートである。

【図９】銀行のキャッシュカードなどに本発明の方法を利用した場合の変形例説明図である。図の（ａ）はカードとＡＴＭ（現金自動取引装置）の主要部ブロック図、（ｂ）はその動作説明図である。

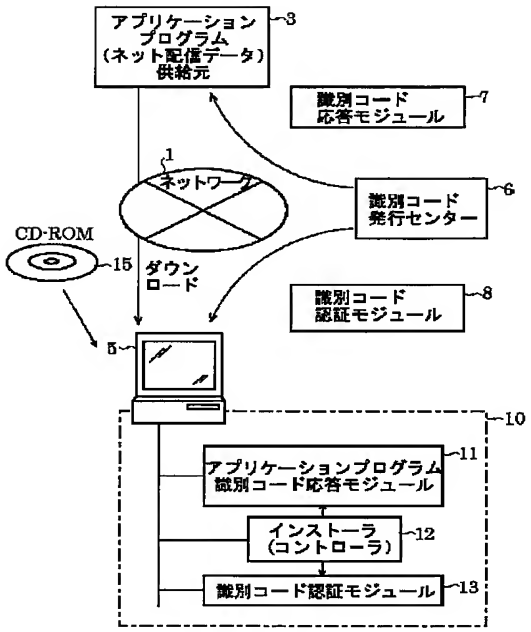
【図１０】図９に示したカードを使用したＡＴＭの動作を説明するためのフローチャートである。

【図１１】本発明の方法をコンピュータのオペレーティングシステムに使用した場合の別の実施例を示すブロック図である。

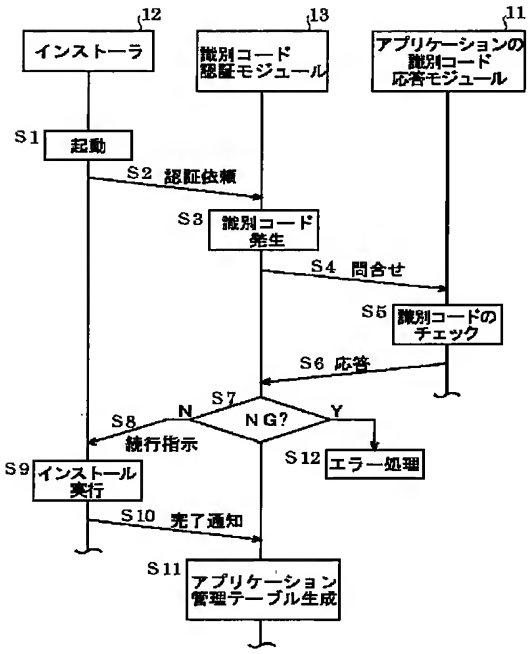
【符号の説明】

１　ネットワーク
３　アプリケーションプログラム供給元
５　端末
６　識別コード発行センター
７　識別コード応答モジュール
８　識別コード認証モジュール
１１　アプリケーションプログラム識別コード応答モジュール
１２　インストーラ
１３　識別コード認証モジュール

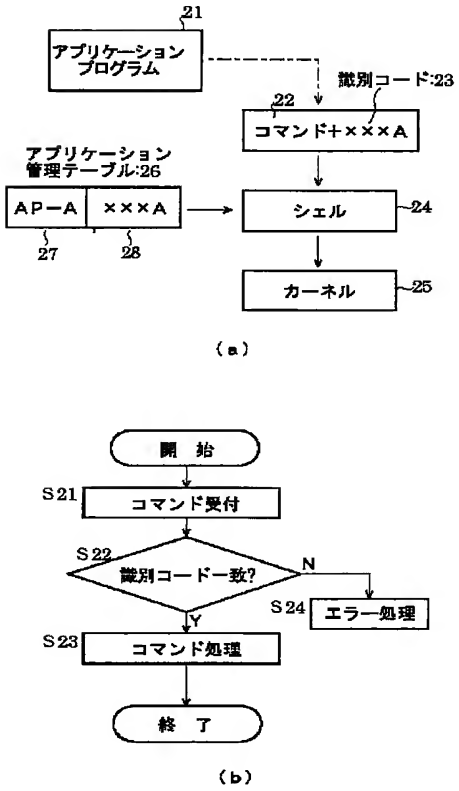
【図１】


アプリケーション
プログラム
(ネット配信データ)
供給元
3
識別コード
応答モジュール
7
1
ネットワーク
識別コード
発行センター
6
CD-ROM
15
ダウン
ロード
識別コード
認証モジュール
8
5
10
アプリケーションプログラム
識別コード応答モジュール
11
インストーラ
(コントローラ)
12
識別コード認証モジュール
13

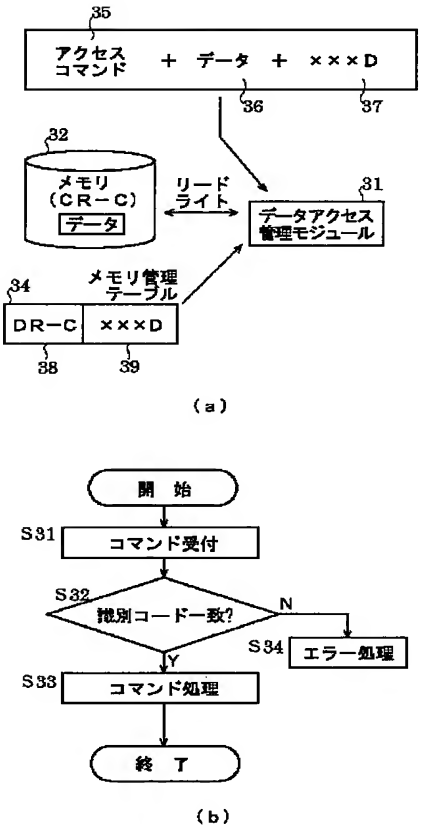
【図２】


12
インストーラ
13
識別コード
認証モジュール
11
アプリケーションの
識別コード
応答モジュール
S1
起動
S2 認証依頼
S3
識別コード
発生
S4 問合せ
S5
識別コードの
チェック
S6 応答
S7
NG?
N
Y
S8
続行指示
S12
エラー処理
S9
インストール
実行
S10 完了通知
S11
アプリケーション
管理テーブル生成

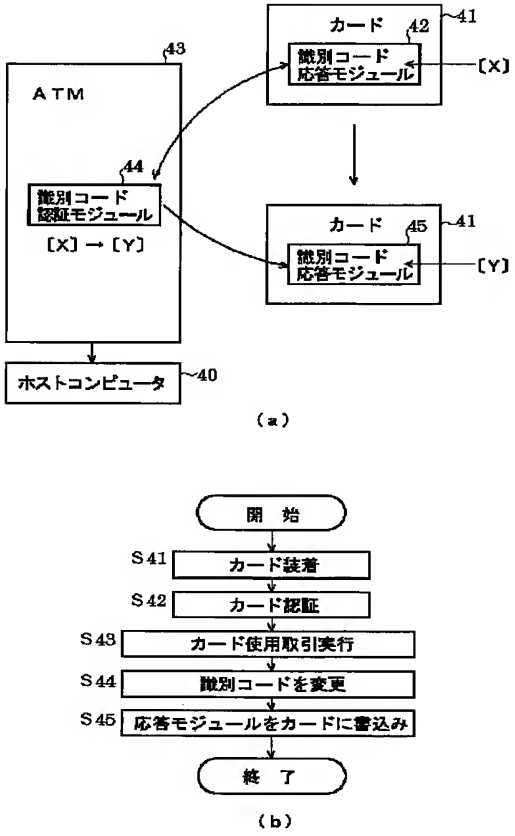
【図３】


21
アプリケーション
プログラム
識別コード:23
22
コマンド+×××A
アプリケーション
管理テーブル:26
AP−A
×××A
27
28
シェル
24
カーネル
25
(a)
開 始
S21
コマンド受付
S22
識別コード一致?
N
S24
エラー処理
Y
S23
コマンド処理
終 了
(b)

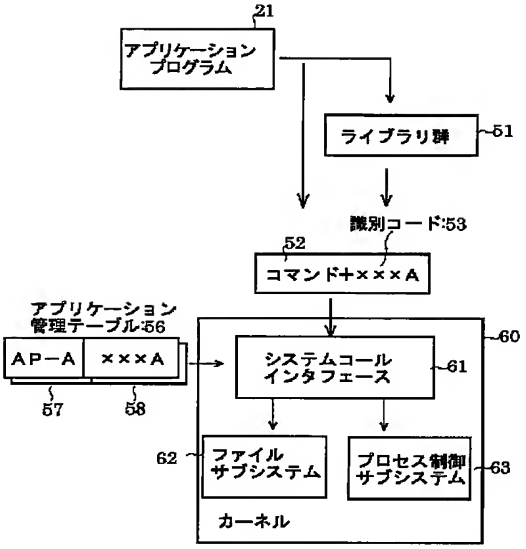
【図４】


35
アクセス
コマンド
＋ データ ＋ ×××D
36
37
32
メモリ
(CR−C)
データ
リード
ライト
31
データアクセス
管理モジュール
メモリ管理
テーブル
34
DR−C
×××D
38
39
(a)
開 始
S31
コマンド受付
S32
識別コード一致?
N
S34
エラー処理
Y
S33
コマンド処理
終 了
(b)

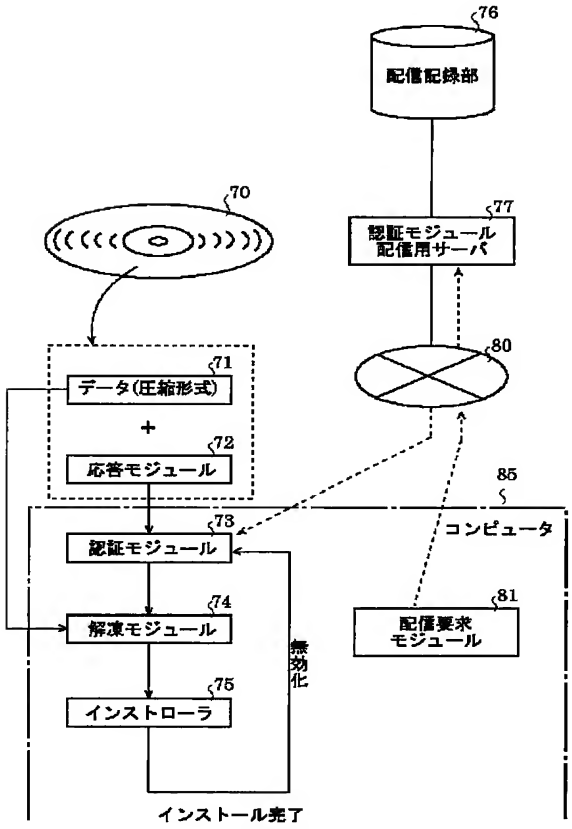
【図５】


カード
42
41
識別コード
応答モジュール
〔X〕
43
ATM
44
識別コード
認証モジュール
〔X〕→〔Y〕
カード
45
41
識別コード
応答モジュール
〔Y〕
ホストコンピュータ
40
(a)
開 始
S41
カード装着
S42
カード認証
S43
カード使用取引実行
S44
識別コードを変更
S45
応答モジュールをカードに書込み
終 了
(b)

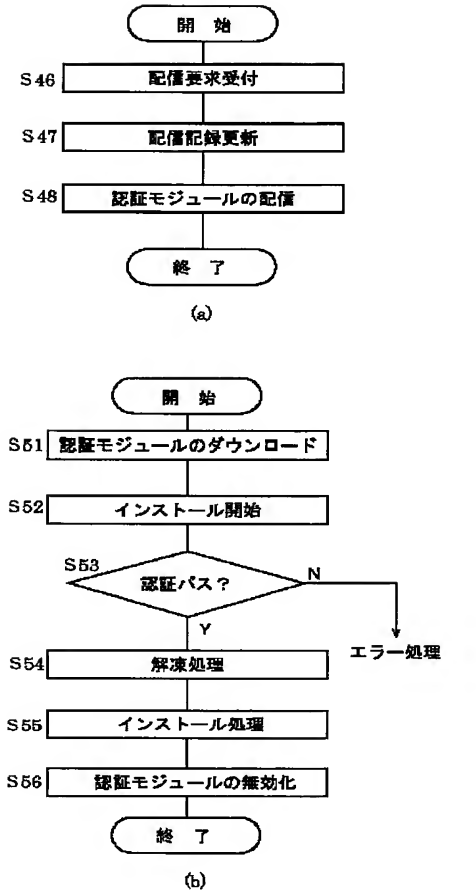
【図６】


21
アプリケーション
プログラム
ライブラリ群
51
識別コード:53
52
コマンド+×××A
アプリケーション
管理テーブル:56
AP−A
×××A
57
58
システムコール
インタフェース
61
60
62
ファイル
サブシステム
プロセス制御
サブシステム
63
カーネル

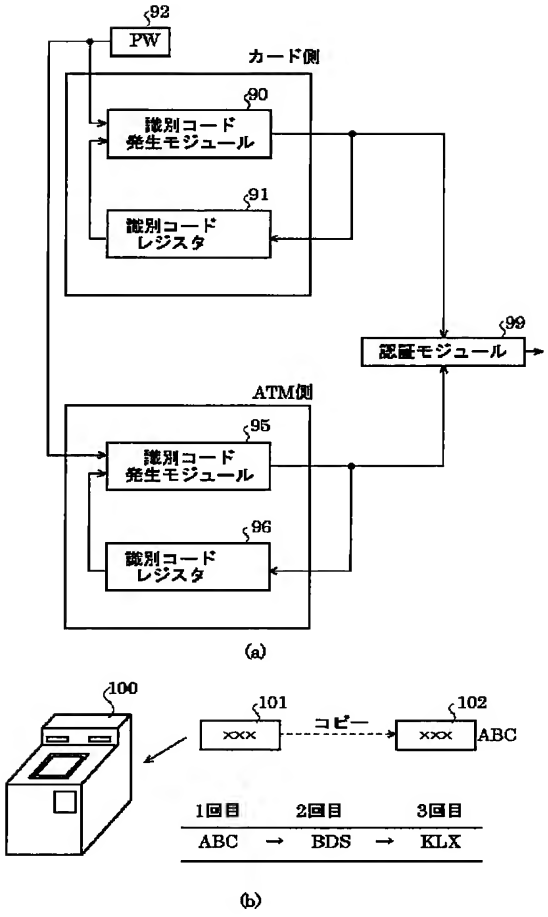
【図７】


76
配信記録部
70
77
認証モジュール
配信用サーバ
80
71
データ(圧縮形式)
+
72
応答モジュール
85
コンピュータ
73
認証モジュール
74
解凍モジュール
81
配信要求
モジュール
無効化
75
インストーラ
インストール完了

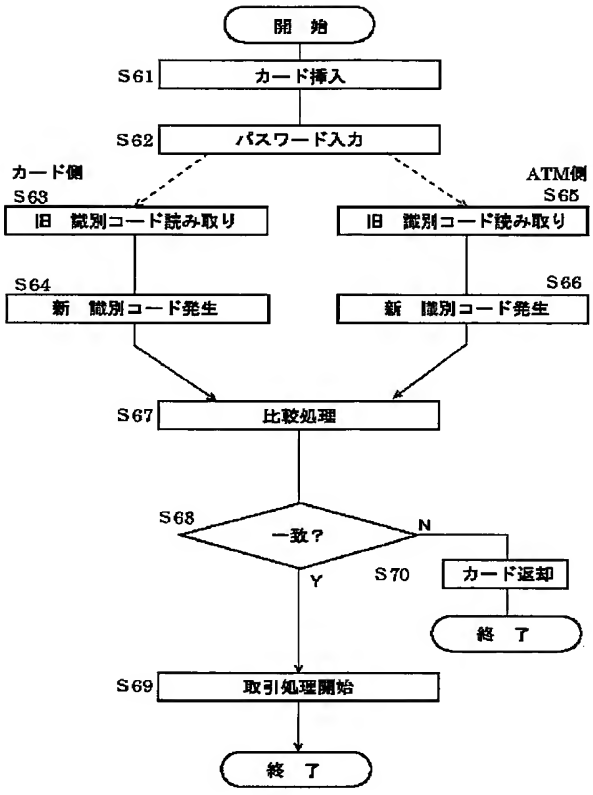
【図８】


開　始
S46
配信要求受付
S47
配信記録更新
S48
認証モジュールの配信
終　了
(a)
開　始
S51
認証モジュールのダウンロード
S52
インストール開始
S53
認証パス？
N
Y
エラー処理
S54
解凍処理
S55
インストール処理
S56
認証モジュールの無効化
終　了
(b)

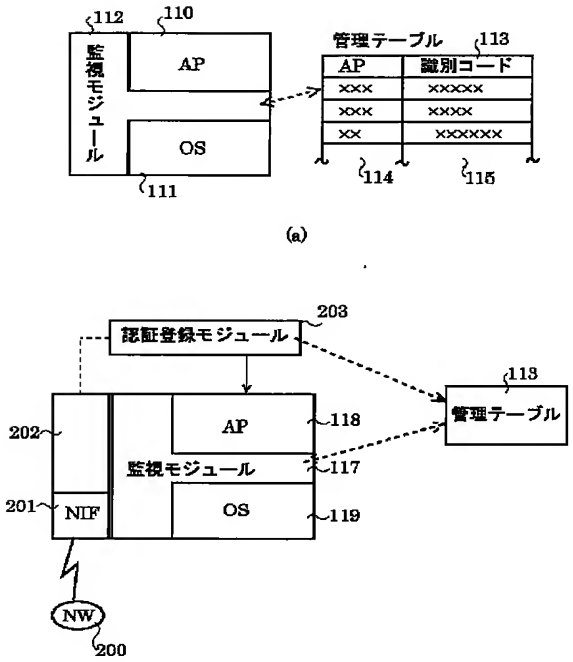
【図９】


92
PW
カード側
90
識別コード
発生モジュール
91
識別コード
レジスタ
99
認証モジュール
ATM側
95
識別コード
発生モジュール
96
識別コード
レジスタ
(a)
100
101
×××
コピー
102
×××
ABC
1回目
2回目
3回目
ABC
→
BDS
→
KLX
(b)

【図１０】


開　始
S61
カード挿入
S62
パスワード入力
カード側
S63
旧　識別コード読み取り
ATM側
S65
旧　識別コード読み取り
S64
新　識別コード発生
S66
新　識別コード発生
S67
比較処理
S68
一致？
N
Y
S70
カード返却
終　了
S69
取引処理開始
終　了

【図１１】


112
110
監視モジュール
AP
OS
111
管理テーブル
113
AP
識別コード
×××
×××××
××××
××
××××××
114
115
(a)
203
認証登録モジュール
113
管理テーブル
202
AP
118
監視モジュール
117
201
NIF
OS
119
NW
200
(b)